

Appendix C

Microsoft Windows NT 3.51 Security Checklist

Topic: AUDIT

SubTopic:

Objective 14

Ensure the audit subsystem is enabled.

Rationale:

UNIX maintains a number of log files that keep track of when users log in and which commands they run. These log files form the basis of UNIX's auditing system. Auditing can be enabled or disabled. It should always be enabled for a secure system.

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

In the "Program Manager", in the "Administrative Tools" group, select the "User Manager" icon. Select "Policies", "Audit" from the menu.

Expected Results:

The "Audit These Events" radio button is selected and some events flags are selected.

Comments:

Auditing provides accountability. This setting is prerequisite to auditing of specific events.

Topic: AUDIT

SubTopic:

Objective 15

Ensure audit is correctly configured and collects the required audit events (login and logout, use of privileged commands, application and session initiation, use of print command, DAC permission modification, export to media...).

Rationale:

DII COE SRS Requirement:

3.2.2.5 At a minimum, the following audit events shall be audited:

3.2.2.5.1 Login (unsuccessful and successful) and Logout (successful)

3.2.2.5.2 Use of privileged commands (unsuccessful and successful)

3.2.2.5.3 Application and session initiation (unsuccessful and successful)

3.2.2.5.4 Use of print command (unsuccessful and successful)

3.2.2.5.5 Discretionary access control permission modification (unsuccessful and successful)

3.2.2.5.6 Export to media (successful)

3.2.2.5.7 Unauthorized access attempts to files (unsuccessful)

3.2.2.5.8 System startup and shutdown (unsuccessful and successful).

Test Actions:

Step: 1

Required Action:

In the "Program Manager", in the "Administrative Tools" group, select the "User Manager" icon. Select "Policies", "Auditing" from the menu.

Expected Results:

The "Audit These Events" radio button is selected.

The "Use of User Rights" Failure checkbox is checked

The "Restart, Shutdown, and System" Success and Failure checkboxes are checked.

Comments:

Auditing provides accountability. This setting is prerequisite to auditing of specific events.

Note: If "System" is selected for auditing, then either "login/logoff" or "process tracking" must also be selected; otherwise "System" will not take effect.

Step: 2

Required Action:

In the "Program Manager", in the "Main" group select the "File Manager" icon. Select the root directory, and then select "Security", "Auditing" from the menu.

Expected Results:

The group "Everyone" is displayed in the "Name" listbox. The "Restart, Shutdown, and System" Success and Failure checkboxes are checked for the group "Everyone". The "Change Permissions" Success and Failure checkboxes are checked for the group "Everyone". The "Take ownership" Success and Failure checkboxes are checked for the group "Everyone". The "Write" and "Delete" "Success" checkbox is checked for the group "Everyone" for critical directories and files, including the system files referenced earlier, other system files, application files, and user files as determined by the site administrator.

Comments:

Note: One problem is that if you audit write access you also audit SYNCHRONIZE. For many files, most notably for system files such as kernl386.exe, this generates an audit message under normal operation. Therefore you need to choose between generating too many audit messages and not auditing changes to critical files.

Topic: AUDIT

SubTopic:

Step: 3

Required Action:

Verify that significant changes to selected Registry keys is audited.

Use the Registry Editor (regedt32.exe) - the Registry Editor can be located using the File Manager and selecting the "WINNT35/system32" directory, then launching the "regedt32.exe" program by double clicking on it. Select HKEY_LOCAL_MACHINE/Software/Program Groups window and then select "Security", "Auditing" menu choice.

Expected Results:

Significant changes are audited.

Comments:

Topic: AUDIT

SubTopic:

Objective 196

Verify the system is capable of detecting when the audit file reaches a configurable threshold and audit records are not lost if this threshold is reached. If the audit file becomes full, verify the system is shutdown until the audit data is archived.

Rationale:

DII COE SRS Requirement:

3.2.2.1.3 The COE shall be capable of detecting when the audit trail reaches a configurable threshold (i.e., % of capacity), ensuring that audit data is not lost, and maintaining system availability.

Test Actions:

Step: 1

Required Action:

In the "Program Manager", in the "Administrative Tools" group, select the "Event Viewer" icon. Select "Log", "Security" from the menu. Select "Log", "Log Settings ... " from the menu. In the "Event Log Settings" window, verify the "Maximum Log Size" entry.

Expected Results:

The "Maximum Log Size" entry is set to at least 2 MB.

Comments:

To ensure that system availability is maintained, verify that the security (audit) log is directed to a large, reliable storage device.

Step: 2

Required Action:

In the "Program Manager", in the "Administrative Tools" group, select the "Event Viewer" icon. Select "Log", "Security" from the menu. Select "Log", "Log Settings ... " from the menu. In the "Event Log Settings" window, verify that "Do Not Overwrite Events" is selected.

Expected Results:

The "Event Log Wrapping" choice "Do Not Overwrite Events" is selected.

Comments:

Topic: AUDIT

SubTopic: Archival of Audit Data

Objective 27

Verify the system provides a configurable capability to archive audit data.

Rationale:

DII COE SRS Requirement:

3.2.2.1.4 The COE shall provide a configurable capability to archive audit data.

Test Actions:

Step: 1

Required Action:

In the "Program Manager", in the "Administrative Tools" group, select the "Event Viewer" icon. Select "Log", "Security" from the menu. Select "Log", "Log Settings ... " from the menu. Select the "Save As ... " choice from the "Log" menu item.

Expected Results:

A dialogbox appears allowing the saving of the log to an administrator selected location.

Comments:

The audit log can get full; regular backups of the audit trail will avoid shutdown of the system.

Topic: AUDIT

SubTopic:

Objective 197

Verify required audit events are recorded in the audit log (login and logout, use of privileged commands, application and session initiation, use of print command, DAC modification , export to media, unauthorized access attempts to files . . .).

Rationale:

DII COE SRS Requirement:

3.2.2.5 At a minimum, the following audit events shall be audited:

3.2.2.5.1 Login (unsuccessful and successful) and Logout (successful)

3.2.2.5.2 Use of privileged commands (unsuccessful and successful)

3.2.2.5.3 Application and session initiation (unsuccessful and successful)

3.2.2.5.4 Use of print command (unsuccessful and successful)

3.2.2.5.5 Discretionary access control permission modification (unsuccessful and successful)

3.2.2.5.6 Export to media (successful)

3.2.2.5.7 Unauthorized access attempts to files (unsuccessful)

3.2.2.5.8 System startup and shutdown (unsuccessful and successful).

Test Actions:

Step: 1

Required Action:

In the "Program Manager", in the "Administrative Tools" group, select the "Event Viewer" icon. Select "Log", "Security" from the menu. Verify that the Security log contains all required events.

Expected Results:

The Security log contains all required events.

Comments:

Topic: AUDIT

SubTopic: Protection of Audit Data

Objective 25

Verify the audit data is protected by the system so that access to it is limited to only those authorized to view the audit data.

Rationale:

DII COE SRS Requirement:

3.2.2.1.1 The audit data shall be protected by the system so that access to it is limited to those who are authorized to view audit data.

Test Actions:

Step: 1

Required Action:

In the "Program Manager", in the "Main" group select the "File Manager" icon. Select the "<SYSTEMROOT>\SYSTEM32\CONFIG" directory. Then select each of the following files, and select "Security", "Permissions ..." from the menu:

SysEvent.Evt

SecEvent.Evt

AppEvent.Evt

Expected Results:

Each of the files show the following permissions:

Administrators: Full Control

SYSTEM: Full Control

Comments:

The audit log should be protected.

Step: 2

Required Action:

Verify that the security (audit) log is maintained on a physically protected system, such as the site's domain controller. Use a third-party audit tool, on a regular basis, to copy the Security log to a physically protected system.

Expected Results:

The audit log is maintained on a physically protected system.

Comments:

The audit log should be protected.

Topic: AUDIT

SubTopic: Audit Reduction

Objective 24

Determine if an audit reduction capability exists. This capability can be either OS provided or an add-on product.

Rationale:

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

Interview the System Administrator to determine if audit data is reviewed and if so, if an audit reduction utility is used.

Expected Results:

Audit data is reviewed and an audit reduction tool is utilized to aid in the review.

Comments:

The native Windows NT audit reduction capability does not provide the best possible analysis of large audit logs.

Topic: Availability

SubTopic: Emergency Repair Disk

Objective 163

Verify that a current emergency repair disk has been created, updated, and is protected with an appropriate password.

Rationale:

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

Verify that a current emergency repair disk is available for each Windows NT system. Interview the System Administrator and check the creation date of the disk.

Expected Results:

The System Administrator creates a current emergency repair disk regularly. The disk is labeled with the system name and the date on the repair disk is less than six months old.

Comments:

Windows NT uses the emergency repair disk to recover from errors and allows recovery if the system should become so damaged that it cannot be booted. The emergency repair disk provides full access to all system components and data, therefore it should be protected appropriately.

Topic: DAC

SubTopic:

Objective 58

Verify a Deadman Timeout function locks a user's terminal if input devices have been idle for a configurable period of time (default 5 minutes) and that users are required to re-authenticate themselves to unlock a locked terminal.

Rationale:

DII COE SRS Requirement:

3.2.4.12 The COE shall provide a deadman function that locks the user's terminal if user input devices have been idle for longer than a configurable time period.

3.2.4.12.1 The configurable time period shall default to 5 minutes.

3.2.4.12.2 Any user input device may be used to restore a locked terminal.

3.2.4.12.3 The specific input value (whether from keyboard, mouse, or other pointer) used to activate the function that restores the locked terminal shall be ignored except to activate the function.

Test Actions:

Step: 1

Required Action:

Verify that a screen saver is enabled for all accounts by interviewing the system administrator and determining that either mandatory profiles that enforce use of a password protected screensaver, or a training program to train users to use screensavers with password protection are in use.

Expected Results:

Mandatory profiles that enforce use of a password protected screensaver, or a training program to train users to use screensavers with password protection are in use.

Comments:

Train users NOT to change the screen saver settings that they are given by default. This protects against a user account from being used by an unauthorized person if a user steps away from the system.

A mandatory profile can enforce the screensaver security policy as well as other security policies for users. Mandatory profiles are discussed in objective 286.

Step: 2

Required Action:

Verify that new user accounts are set up with screen saver enabled and set to require a password to clear. Set up a new account and verify that the screen saver is enabled.

Expected Results:

Screen saver is automatically enabled with the creation of new accounts.

Comments:

The system should be locked when unattended.

Topic: DAC

SubTopic:

Objective 60

Verify DAC mechanisms are used to restrict access by general users to input/output (I/O) devices, such as floppy disks and tape drives, and that the SGSO has the capability to specify which users may access I/O devices.

Rationale:

DII COE SRS Requirement:

3.2.4.11 The COE shall be capable of using DAC mechanisms to restrict access by general users to input/output (I/O) devices, such as floppy disks and tape drives.3.2.4.11.1 The COE shall provide a capability for the SGSO to specify which users may access I/O devices.

Test Actions:

Step: 1

Required Action:

Verify that access to floppy disks is restricted to the user currently logged on.

In the "Program Manager", in the "Administrative Tools" group, select the "Regedt32" icon. Click on the window "HKEY_LOCAL_MACHINE" and the folder "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows-NT\CurrentVersion\Winlogon".

Expected Results:

The "AllocateFloppies" key is set to "1".

Comments:

By default, "AllocateFloppies" will not be in the registry key. To add "AllocateFloppies" see configuration steps.

Remote access to the floppy drive is rarely needed. A process can remain running in the background after the user logs off and then access the floppy drive while another user is logged on.

Step: 2

Required Action:

Verify that access to CD-ROM disks is restricted to the user currently logged on.

In the "Program Manager", in the "Administrative Tools" group, select the "Regedt32" icon. Click on the window "HKEY_LOCAL_MACHINE" and the folder "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms".

Expected Results:

The "AllocateCDRom" key is set to "1".

Comments:

This should be done if the system is not intended to be a CD-ROM server. If remote access is enabled the user who inserts a CD-ROM may not be aware that other users can read it and may insert a CD-ROM that is not intended for general access. In addition, a process can remain running in the background after the user logs off, and access the CD-ROM drive while another user is logged on.

Topic: DAC

SubTopic:

Objective 64

Verify normal users cannot bypass mechanisms to obtain privileges that are allowed only to privileged users (e.g., the SSA or root).

Rationale:

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

In the "Program Manager", in the "Administrative Tools" group select the "User Manager" icon. Select "Policies", "User Rights" from the menu. Select the "Show Advanced Rights" checkbox in the lower left corner of the "User Rights Policy" form. Select "Create Token" from the "Right" dropdown list.

Expected Results:

No user or group account is listed in the "Grant to" listbox.

Comments:

These rights are used by the OS TCB. They have the power to subvert the security of the operating system.

Step: 2

Required Action:

In the "Program Manager", in the "Administrative Tools" group select the "User Manager" icon. Select "Policies", "User Rights" from the menu. Select the "Show Advanced Rights" checkbox in the lower left corner of the "User Rights Policy" form. Select the "TCB Privilege" from the "Right" dropdown list.

Expected Results:

No user or group account is listed in the "Grant to" listbox.

Comments:

These rights are used by the OS TCB. They have the power to subvert the security of the operating system.

Step: 3

Required Action:

In the "Program Manager", in the "Administrative Tools" group select the "User Manager" icon. Select "Policies", "User Rights" from the menu. Select the "Show Advanced Rights" checkbox in the lower left corner of the "User Rights Policy" form. Select "Assign Primary Token" from the "Right" dropdown list.

Expected Results:

No user or group account is listed in the "Grant to" listbox.

Comments:

These rights are used by the OS TCB. They have the power to subvert the security of the operating system.

Topic: DAC

SubTopic: Least Privilege

Objective 284

Verify that users and groups available on the system have the appropriate privileges.

Rationale:

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

In the "Program Manager", in the "Administrative Tools" group, select the "User Manager" icon. Select "Policies", "User Rights" from the menu. Select the "Log on locally" right and check the groups this right is assigned to. In the "Grant To" box verify that the groups Everyone and Guests are not listed.

Expected Results:

The groups "Everyone" and "Guests" are not listed in the "Grant To" box.

Comments:

"Guest" is a member of group "Everyone" and this is one of several steps that can be taken to limit access to the system via this unsafe login. Regular users will retain the right to log on locally if the group "Users" is granted the right.

Step: 2

Required Action:

In the "Program Manager", in the "Administrative Tools" group, select the "User Manager" icon. Select "Policies", "User Rights" from the menu. Select the "Show Advanced Rights" checkbox in the lower left corner of the "User Rights Policy" form. Select each right one at a time from the "Right" dropdown list and verify the users granted each right.

Expected Results:

The rights for the "Users" group have been restricted to the "Log on locally", "Shut down the system", and, if needed for operational reasons, "Access this computer from network" rights.

Comments:

These are the only rights needed for operational work, and by the principle of least privilege no additional rights should be granted. Depending on the operational use of the system, the right "Access this computer from network" may be needed, but this right should not be granted unless it is needed.

Step: 3

Required Action:

In the "Program Manager", in the "Administrative Tools" group, select the "User Manager" icon. Select "Policies", "User Rights" from the menu. Check the "Show Advanced Rights" checkbox in the lower left corner of the "User Rights Policy" form. Select the "Debug programs" right from the "Right" dropdown list and view the users granted this right. Verify that no user, not even "Administrator", has the "Debug programs" right.

Expected Results:

No User is listed in the "Grant to" listbox.

Comments:

This right should NOT be enabled if the system is a production system. Users with the "Debug Programs" right can access system memory where sensitive information, such as passwords, may be cached.

Topic: DAC
SubTopic: Least Privilege

Step: 4

Required Action:

In the "Program Manager", in the "Administrative Tools" group select the "User Manager" icon. Select "Policies", "User Rights" from the menu. Select the "Show Advanced Rights" checkbox in the lower left corner of the "User Rights Policy" form. Select the "Logon as a service" right from the "Right" dropdown list and view the users granted the chosen right. Verify that no user, not even Administrator, has the "Logon as a service" right.

Expected Results:

No User is listed in the "Grant to" listbox.

Comments:

This right allows a process to register as a system service. Since services are usually installed using the "Services" control panel, this right is not needed.

Step: 5

Required Action:

Verify that third party services run under an account in which rights have been tailored to include only those rights essential to allow the service to perform its function. In addition, no service should run under the "Administrator" account.

Expected Results:

Comments:

Topic: DAC

SubTopic: Permissions

Objective 257

Verify that permissions on all "temp" directories are set correctly.

Rationale:

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

From the "Program Manager", in the "Main" group, select the "Control Panel" and then double-click on the "System" icon. Determine what the Temporary directory is from the "User Environment Variable" listbox. In the "Program Manager", in the "Main" group, select the "File Manager" icon. Select each TEMP directory listed and then select "Security", "Permissions" from the menu.

Expected Results:

Permissions on all TEMP directories are set to:

SYSTEM, Full control
Administrators, Full control
CREATOR/OWNER, Full control
Everyone, Add permission only
Users, Add permission only

Comments:

A TEMP directory is one defined by the current environment variable "TEMP." TEMP directories are used by many applications as a repository for temporary files containing data that should be protected from access by unauthorized users.

Topic: DAC

SubTopic: Registry Keys

Objective 258

Verify that all Registry key ACLs used to support applications have been set correctly.

Rationale:

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

Verify that ACLs on all Registry keys used to support applications not needed by "Guest" have been set to deny write and execute access for the group "Everyone", but have granted the "write" and "execute" accesses for the group "Users". Note: This should only be done if the group "Everyone" previously had "write" and "execute" access.

Expected Results:

The ACLs on all Registry keys used to support applications not needed by "Guest" have been set to deny write and execute access for the group "Everyone", but have granted the "write" and "execute" accesses for the group "Users".

Comments:

This should be done if some applications depend on the availability of the "Guest" account and the applications cannot be rewritten to not depend on this account. This setting will limit to some degree the damage that can be done if an attacker accesses the system using the "Guest" account.

A utility such as "DumpACL" can be used to dump the ACLs for the entire registry. Even using this utility, this task will be labor intensive and require determining which applications do not require the "Guest" account. DumpACL can be obtained from "<http://www.somarsoft.com>".

Topic: FILE SYS SEC

SubTopic: Permissions

Objective 66

Ensure the file systems are configured correctly and securely.

Rationale:

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

In the "Program Manager", in the "Administrative Tools" group, select the "Disk Administrator" icon. Ensure that the "File Type" for each disk listed is "NTFS".

Expected Results:

The file system type on all hard drives listed is NTFS.

Comments:

The NTFS file system is the only file system that supports DAC for file system objects.

Step: 3

Required Action:

In the "Administration Tools" group, select the "Disk Administrator" icon. Select "Partition" from the menu and verify that the "Secure System Partition" option is enabled.

Expected Results:

The "Secure System Partition" should be selected. This will restrict access of the FAT boot partition to "Administrators" only and protects the system files on the FAT boot partition.

Comments:

This should be done if the system is a RISC system.

Topic: FILE SYS SEC

SubTopic: Permissions

Objective 67

Verify file permissions are set appropriately throughout the file system.

Rationale:

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

In the "Program Manager", in the "Main" group, select the "File Manager" icon. Select the "C:\ - NTFS" directory and then select "Security", "Permissions" from the menu. Verify the permissions on the C:\ directory.

Expected Results:

The permissions on the C:\ directory are set to:

CREATOR/OWNER, Full Control
Everyone, Add and Read
System, Full Control
Administrators, Full Control

These permissions allow the group "Everyone" to create and add new files and directories, and by default, only the creator, "System", or "Administrators" accounts will have access to the newly created files.

Comments:

These settings protect system files in the root directory, such as autoexec.bat, from being deleted and replaced with an attacker's version.

Step: 2

Required Action:

In the "Program Manager", in the "Main" group, select the "File Manager" icon. Select the "C:\Boot.ini" file and then select "Security", "Permissions" from the menu. Verify the file permissions. Repeat this procedure on the "C:\Ntldetect.com" and "C:\Ntldr" files.

Expected Results:

The file permissions are set to:

Administrators: Full Control
SYSTEM: Full Control

Comments:

These settings are specified for C2 configuration for Intel platforms.

Step: 3

Required Action:

In the "Program Manager", in the "Main" group, select the "File Manager" icon. Select the "C:\AUTOEXEC.BAT" file and then select "Security", "Permissions" from the menu. Verify the file permissions. Repeat this procedure for the "C:\CONFIG.SYS" file.

Expected Results:

The file permissions are set to:

Everyone: Read
Administrators: Full Control
SYSTEM: Full Control

Topic: FILE SYS SEC

SubTopic: Permissions

Comments:

These settings are specified for C2 configuration on Intel platforms, and protect the operating system from unauthorized modification.

Step: 4

Required Action:

In the "Program Manager", in the "Main" group, select the "File Manager" icon. In the File Manager, select the "C:\WINNT35\" directory and then select "Security" , "Permissions" from the menu. Verify the directory permissions.

Expected Results:

The permissions are set to:

Administrators: Full Control
CREATOR OWNER: Full Control
Everyone: Read
SYSTEM: Full Control
Users: Change

The groups "Everyone" or "Users" do NOT have "Delete" access.

Comments:

These settings protect the operating system from unauthorized modification. Use the settings recommended here, then relax permissions as needed and approved by the responsible security officer. Using these settings, only administrators will be able to install most applications, and users of 16-bit applications may not be able to customize options. This is not as restrictive as is desirable, since it gives the "Users" group the "Change access" right to all "*.ini" files although this right may not be needed. Identifying which applications need the "Change access" right to their ".ini" files is difficult to do with complete accuracy.

Note: c2config.exe from the Windows NT Resource Kit for NT 3.51 includes a secure configuration for the system directories; the DACLs provided are less restrictive, and therefore more risky, than those recommended here.

Step: 5

Required Action:

In the "Program Manager", in the "Main" group, select the "File Manager" icon. In the File Manager, select the "C:\WINNT35\" directory and then select "Security" , "Permissions" from the menu. Verify the permissions on all "*.ini" files.

Expected Results:

The permissions are set to:

Administrators: Full Control
CREATOR OWNER: Full Control
Everyone: Read
SYSTEM: Full Control
Users: Change

The groups "Everyone" or "Users" do NOT have "Delete" access.

Topic: FILE SYS SEC**SubTopic: Permissions*****Comments:***

These settings protect the operating system from unauthorized modification. Use the settings recommended here, then relax permissions as needed and approved by the responsible security officer. Using these settings, only administrators will be able to install most applications, and users of 16-bit applications may not be able to customize options. This is not as restrictive as is desirable, since it gives the "Users" group the "Change access" right to all "*.ini" files although this right may not be needed. Identifying which applications need the "Change access" right to their ".ini" files is difficult to do with complete accuracy.

Note: c2config.exe from the Windows NT Resource Kit for NT 3.51 includes a secure configuration for the system directories; the DACLs provided are less restrictive, and therefore more risky, than that recommended here. Some applications and services that are used at a site may require greater access than those recommended here. Each relaxation of permissions should be analyzed to determine its security impact.

Step: 6***Required Action:***

In the "Program Manager", in the "Main" group, select the "File Manager" icon. In the File Manager, select the "C:\WINNT35\SYSTEM" directory and then select "Security", "Permissions" from the menu. Verify the permissions on this directory.

Expected Results:

The permissions are set to:

Administrators: Full Control
CREATOR OWNERS Full Control
Everyone: Read
SYSTEM: Full Control

The groups "Everyone" or "Users" do NOT have "Delete" access.

Comments:

These settings are specified for C2 configuration and protect the operating system from unauthorized modification. Relax permissions as needed and approved by the responsible security officer.

Note: c2config.exe from the Windows NT Resource Kit for NT 3.51 includes a secure configuration for the system directories but the DACLs provided are less restrictive, and therefore more risky than recommended here. Using these settings, only administrators will be able to install most applications, and users of 16-bit applications may not be able to customize options. If these settings prove too restrictive, users may be given the "Change" permission.

Step: 7***Required Action:***

In the "Program Manager", in the "Main" group, select the "File Manager" icon. In the File Manager, select the "C:\WINNT35\SYSTEM" directory and then select "Security", "Permissions" from the menu. Verify the permissions on this directory.

Expected Results:

The permissions on this directory are set to:

Administrators: Full Control

CREATOR OWNER: Full Control

Everyone: Read

SYSTEM: Full Control

Topic: FILE SYS SEC

SubTopic: Permissions

Comments:

These settings protect the operating system from unauthorized modification.

Step: 8

Required Action:

In the "Program Manager", in the "Main" group, select the "File Manager" icon. In the File Manager, select the "C:\WINNT35\SYSTEM32\DRIVERS" directory and then select "Security" , "Permissions" from the menu.

Verify the permissions on this directory.

Expected Results:

The permissions on this directory on are set to:

Administrators: Full Control
CREATOR OWNER: Full Control
Everyone: Read
SYSTEM: Full Control

Comments:

These settings are specified for C2 configuration and protect the operating system from unauthorized modification.

Step: 9

Required Action:

In the "Program Manager", in the "Main" group, select the "File Manager" icon. In the File Manager, select the "C:\WINNT35\SYSTEM32\CONFIG" directory and then select "Security" , "Permissions" from the menu.

Verify the permissions on this directory.

Expected Results:

Verify that permissions are set to:

Administrators: Full Control
CREATOR OWNER: Full Control
Everyone: List
SYSTEM: Full Control

Comments:

NOTE: If these settings are propagated to subdirectories, the groups "Everyone" and "Users" will be able to create a profile, but won't be able to read other users' profiles.

Topic: FILE SYS SEC

SubTopic: Permissions

Step: 10

Required Action:

In the "Program Manager", in the "Main" group, select the "File Manager" icon. In the File Manager, select the "C:\WINNT35\SYSTEM32\SPOOL" directory and then select "Security" , "Permissions" from the menu.

Verify the permissions on this directory.

Expected Results:

The permissions are set to:

Administrators: Full Control
CREATOR OWNER: Full Control
Everyone: Read
Power Users: Change
SYSTEM: Full Control

Comments:

These settings are specified for C2 configuration.

Step: 11

Required Action:

In the File Manager, select the "C:\WINNT35\SYSTEM32" directory. Verify that the "OS2" directory does not exist.

Expected Results:

This directory does NOT exist.

Comments:

OS/2 commands are not needed, and any unnecessary complexity of the operating system potentially increases vulnerability.

Step: 12

Required Action:

In the "Program Manager", in the "Main" group, select the "File Manager" icon. In the File Manager, select the shared directory used as a central repository for user profiles, and then select "Security" , "Permissions" from the menu.

Verify the permissions on the directory.

Expected Results:

The permissions on the shared directory used as a central repository for user profiles are set to:

Administrators: Full Control
CREATOR OWNER: Full Control
SYSTEM: Full Control
Everyone: Add

Comments:

Profiles can contain sensitive information. This setting protects against attacks based on substituting or copying a profile.

Topic: FILE SYS SEC
SubTopic: System Shutdown

Objective 84

Verify if the machine is a server, domain controller, or it's availability is otherwise critical, it cannot be shutdown without first logging on.

Rationale:

{need to mention physical security - anyone can pull the plug or type "L1-A" - you can ensure that no accounts exist on the Unix platform with "shutdown, halt,..etc" for a shell}

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

Verify the system cannot be shut down without logging on.

In the "Program Manager" in the "Administration Tools" group, select the "Regedt32" icon. Click on the HKEY_LOCAL_MACHINE window to bring it to the front and check the "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ShutdownWithoutLogon" registry key.

Expected Results:

The "HKEY_LOCAL_MACHINE\Software\Microsoft\ WindowsNT\CurrentVersion\Winlogon\ ShutdownWithoutLogon" registry key is set to zero.

Comments:

Only authorized users should be allowed to shut down critical systems therefore this should be done if the machine is a server or domain controller, or it's availability is otherwise critical. The risk of someone simply pulling the plug is less than the risk of someone shutting down the system from the login prompt screen.

Topic: FILE SYS SEC

SubTopic: Permissions

Objective 259

Verify that permissions on the "Repair" function are set correctly.

Rationale:

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

In the "Program Manager", in the "Main" group, select the "File Manager" icon. Select the "C:\WINNT35\REPAIR" directory and then select "Security", "Permissions" from the menu. Verify the directory permissions.

Expected Results:

The permissions are set to:

Administrators, Full Control

Comments:

This setting is specified for C2 configuration. Running the repair function may give access to all data on the system, therefore access to this function should be tightly controlled.

Topic: FILE SYS SEC

SubTopic: Permissions

Objective 260

Verify that permissions on the backup program are set correctly.

Rationale:

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

In the "Program Manager", in the "Main" group, select the "File Manager" icon. Select the "C:\WINNT35\SYSTEM32\NTBACKUP.EXE" file and then select "Security", "Permissions" from the menu.

Verify the file permissions.

Expected Results:

The permissions are set to:

Administrators: Full Control

SYSTEM: Full Control

Comments:

These settings protect the backup program from unauthorized modification.

Topic: FILE SYS SEC

SubTopic: Permissions

Objective 261

Verify that file permissions on all executable files are set correctly.

Rationale:

Trojan horses and many viruses replicate by modifying executable files.

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

Verify that all executable files have read and execute permission but NOT write permission granted to users authorized to execute the program. NOTE: Users specifically authorized to maintain executable files are an exception to this rule.

This test objective can be verified by using the program DumpAcl to generate a report on file system permissions. The resulting report can then be filtered with the string "exe." If any of these executable files are modifiable by the group "Users", go to the File Manager and remove the write permissions on those files for the "Users" group.

Expected Results:

The resulting permissions on all executable files should be:

CREATOR OWNER: Full Control

Everyone: Read

System: Full Control

Administrators: Full Control

Comments:

Topic: FILE SYS SEC

SubTopic: Permissions

Objective 262

Verify that permissions on directories containing executable files are set correctly.

Rationale:

Necessary to protect executable files, including operating system files, from being replaced by versions containing Trojan Horses.

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

Verify that directories containing executable files deny write permission to all users not specifically authorized to maintain the executables contained in the directory.

In the File Manager select the "C:\WINNT35\SYSTEM32\CONFIG\SOFTWARE" directory. Select "Security" , "Permissions" from the menu. Verify the directory permissions and then repeat the procedure for the following directories:

C:\WINNT35

C:\WINNT35\SYSTEM32

Expected Results:

the permissions on the subdirectories (NOT the files) are:

Administrators: Full Control

CREATOR OWNER: Full Control

Everyone: Read

SYSTEM: Full Control

NOTE: The boxes "Replace Permissions on Subdirectories" or "Replace Permissions on Existing Files" are NOT checked.

Comments:

After new software is installed, check that this security recommendation is still being met and take action if necessary.

In File Manager, search for *.exe, *.bat, and *.com to identify all directories containing executables.

Topic: FILE SYS SEC
SubTopic: System Shutdown

Objective 263

Verify that only privileged users can shutdown, reboot, or restart a system (either locally or remotely).

Rationale:

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

Verify the groups "Everyone" and "Guests" do not have the right to shut down the system:

In the "Program Manager" in the "Administrative Tools" group, select the "User Manager" icon. Select "Policies", "User Rights" from the menu. Select "Shut down the system" from the "Right" pull down menu and verify that the "Users" group IS listed and the groups "Everyone" and "Guests" are NOT.

Expected Results:

The groups "Everyone" and "Guests" are NOT listed for the "Shut down the system" right.

Comments:

This limits the effects that the built-in "Guest" account can have on the system. Normal users may still shutdown the system if the "Users" group is granted this right.

Step: 2

Required Action:

If the machine is a server or domain controller, verify that the "Users" group does not have the right to shut down the system. In the "Program Manager" in the "Administrative Tools" group, select the "User Manager" icon. Select "Policies", "User Rights" from the menu. Select "Shut down the system" from the "Right" pull down menu and verify that the "Users" group is NOT listed.

Expected Results:

The "Users" group is NOT listed for the "Shut down the system" right.

Comments:

This should be done if the machine is a server or domain controller.

Step: 3

Required Action:

Verify that only "Administrators" and "Power Users" may shut down the system from a remote site: In the "Program Manager" in the "Administrative Tools" group, select the "User Manager" icon. Select "Policies", "User Rights" from the menu. In the "User Rights Policy" window select the arrow on the "Right" pull down box and select "Shut down the system". In the "Grant to" portion of the "User Rights Policy" window, verify the "Administrators" and "Power Users" groups are listed.

Expected Results:

The "Administrators" and "Power Users" groups should be listed for this right because it protects availability of the system, yet allows remote control for sites that don't administer their own systems.

Comments:

Topic: FTP

SubTopic:

Objective 132

Determine whether FTP is enabled on the system. If FTP is enabled, verify that it has been securely configured.

Rationale:

The File Transfer Protocol (FTP) allows the user to transfer complete files between systems. ftp is the client program; /etc/ftpd is the server.

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

Attempt to connect to the local host using FTP.

Expected Results:

If successful, then ftp is enabled. See configuration instructions for secure configuration.

Comments:

Topic: FTP

SubTopic: Anonymous FTP

Objective 134

Determine whether anonymous FTP is enabled on the system. If anonymous FTP is enabled, verify that it has been securely configured.

Rationale:

Anonymous FTP allows users who do not have an account on a machine to have restricted access in order to transfer from a specific directory. Because the anonymous FTP feature allows anyone to access the system (albeit in a very limited way), it should not be made available on every host on the network. If anonymous ftp is required, one machine should be chosen (preferably a server or standalone host) on which to allow this service. (Curry, 1990)

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

In the "Program Manager", in the "Main" group, select the "Control Panel" and then double-click the "Network" icon. In the "Installed Network Software" listbox, select "FTP Server" and press the "Configure" button. Verify that the "Allow Anonymous Connections" box is NOT checked.

OR

Attempt to login into the server using the user name "anonymous" and a valid mailname as the password.

Expected Results:

The "Allow Anonymous Connections" box is NOT checked indicating that anonymous FTP is NOT enabled.

OR

the anonymous login attempt does NOT succeed.

Comments:

This must be done if the FTP server must be enabled. Anonymous FTP connections break the trail of accountability from action to user.

Step: 2

Required Action:

If the FTP server must be enabled, verify that a separate partition on an NTFS file system is the only partition to which read or write access is allowed via the FTP server.

In the "Program Manager", in the "Main" group, select the "Control Panel" and then double-click the "Network" icon. In the "Installed Network Software" listbox, select "FTP Server" and press the "Configure" button. Verify that the Home Directory" field contains the name of a separate NTFS partition.

Expected Results:

The Directory listed in the Home Directory field contains the name of a separate NTFS partition that is ONLY used by the FTP server.

Comments:

WinNT 3.51 exports the entire partition containing the FTP home directory. Using a separate partition for the FTP server protects other files on the system from access via FTP.

Topic: FTP

SubTopic: Anonymous FTP

Step: 3

Required Action:

If anonymous FTP is enabled, verify that the Windows NT 3.51 FTP server has been replaced with another, more secure server.

Expected Results:

The Windows NT 3.51 FTP server has been replaced with a more secure server.

Comments:

The default FTP server that ships with NT is a major security headache.

Alternative more secure servers include:

The SSL FTP Server.

The Washington University (at St. Louis, MO) FTP Server.

The Microsoft IIS FTP server

The Microsoft WinNT 4.0 server

The problem is that you can set up your FTP site in c:\ftp, but when a user connects, they can then execute a "cd c:\winnt35\system32", and be in your system directory (subject only to the ACLs that apply to the username under which they connect).

Step: 4

Required Action:

In the "Program Manager", in the "Main" group, select the "Control Panel" and then double-click the "Network" icon. In the "Installed Network Software" listbox, select "FTP Server" and press the "Configure" button. Verify that the FTP user account has been changed from "Guest" to another account that is not a member of any normal user group.

Expected Results:

The anonymous FTP user account has been changed from "Guest" to another account.

Comments:

This should be done if anonymous FTP is turned on.

Limits damage that can be done by a user logging on as the ftp user.

Step: 5

Required Action:

In the "Program Manager", in the "Main" group, select the "Control Panel" and then double-click the "Network" icon. In the "Installed Network Software" listbox, select "FTP Server" and press the "Configure" button. Verify that the "Password" field contains a password.

Expected Results:

The anonymous FTP user account has a password.

Comments:

This should be done if anonymous FTP is turned on.

Prevents attackers from logging in directly using the FTP user account

Topic: HARDWARE/FIRMWARE

SubTopic:

Objective 184

Verify the single user boot or system firmware password is set, and the system is configured such that a password must be entered to boot to a single-user state.

Rationale:

DII COE SRS Requirement:

3.2.12.3 The COE shall be configured such that a password must be entered to boot to a single-user state.

Test Actions:

Step: 1

Required Action:

Verify that the system firmware has been configured to require a password to boot the system. Use procedures provided by the BIOS vendor.

Expected Results:

A password is required to boot the system.

Comments:

This should be done if the option of defining which drives are bootable is not available in the system firmware.

Step: 2

Required Action:

Verify that the system firmware can only be accessed by password and supports an option defining which drives are bootable.

Expected Results:

A password restricts booting the system into a non-secure operating system while still allowing system boots without password.

Comments:

If necessary, upgrade the system BIOS chip. This should be done if the option of defining which drives are bootable is not available in the system firmware.

Step: 3

Required Action:

Verify that the system BIOS chip supports a boot password that is required for both cold and warm boot.

Expected Results:

The system cannot be booted without a password. Makes it more difficult for attackers to boot the system into a non-secure operating system.

Comments:

Some system BIOS chips support a boot password that is required for both a cold and warm boot. This option makes it more difficult for attackers to boot the system into a non-secure operating system. If necessary, upgrade the system BIOS chip.

Topic: I&A

SubTopic:

Objective 108

Verify the system provides the capability to restrict multiple login failures, locks out the userID and prohibits further login if the threshold is reached, sends a notification to the SGSO, and allows the SGSO to restore the locked out userID.

Rationale:

DII COE SRS Requirement:

3.2.1.7 The COE shall provide a capability to restrict multiple login failures.

3.2.1.7.1 If the number of login failures reaches a SGSO configurable threshold (0 through 5), the userID shall be locked and the user shall be prohibited from further login attempts.

3.2.1.7.2 If the number of multiple login failures is set to 0, the capability shall be disabled.

3.2.1.7.3 If a userID is locked, the COE shall send a notification to the SGSO.

3.2.1.7.4 The COE shall provide the SGSO the capability to restore locked userIDs.

Test Actions:

Step: 1

Required Action:

In the "Program Manager", in the "Administrative Tools" group select the "User Manager" icon. Select "Policies", "Account" from the menu. Verify that the number of failed logins before lockout is set to five attempts.

Expected Results:

In the "Account Policy" dialog box the "Lockout after - bad logon attempts" box should be set to five attempts.

Comments:

Five attempts is enough for even the sleepest user to type the password correctly, but is too few for most password-guessing attacks.

Step: 2

Required Action:

In the "Program Manager", in the "Administrative Tools" group select the "User Manager" icon. Select "Policies", "Account" from the menu. Verify that the time period to reset the failed login attempt counter is set to 30 minutes.

Expected Results:

In the "Account Policy" dialog box the "Reset count after - minutes" box is set to 30 minutes.

Comments:

Limits the effectiveness of password guessing attacks.

Step: 3

Required Action:

In the "Program Manager", in the "Administrative Tools" group select the "User Manager" icon. Select "Policies" and then "Account" from the menu. Verify that the delay before automatically reopening account after lockout is set to forever.

Expected Results:

In the "Account Policy" dialog box the "Forever" box in the "Lockout Duration" list box should be checked.

Comments:

This ensures that system administrator must intervene and enforces administration awareness of password-guessing attacks.

Topic: I&A

SubTopic: Accounts

Objective 118

Verify that users that privileged users have a second user account to use for everyday, operational work.

Rationale:

Having a second account limits the damage that can be done by software run by a system administrator engaged in non-administrative activities. For example if a privileged user runs software infected by a virus or Trojan horse using their privileged account, the application may be able to bypass operating system protections.

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

Verify that users that are members of "Administrators" group do not use their accounts for everyday operational work.

Expected Results:

All users with accounts that are members of the "Administrators" group have a second account that is not a member of the "Administrators" group and are trained to use it when not engaged in system administrative work.

Comments:

Topic: I&A

SubTopic: Accounts

Objective 121

Verify that general user accounts do not have administrator privileges.

Rationale:

Limits the damage that can be done by operational software. If some users need a subset of Administrator group rights a group with a subset of administrator rights should be created and users are assigned to it.

Implements rule of least privilege.

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

In the "Program Manager", in the "Administrative Tools" group, select the "User Manager" icon. Review the privileges assigned to the "Users" group.

Expected Results:

The Least possible privileges that allow completion of the mission are granted to the "Users" group.

Comments:

Accounts used for operational work should only be members of the "Users" group and should not have unnecessary rights granted.

Topic: I&A

SubTopic: Password Management

Objective 105

Verify the system enforces individual user accountability, a globally-unique valid userid and password is required for all users to access the system, and the user's identity is associated with all auditable actions performed.

Rationale:

Some sites have installed accounts with names such as "who," "date," "lpq," and so on that execute simple commands. These accounts are intended to allow users to execute these commands without having to log in to the machine. Typically these accounts have no password associated with them, and can thus be used by anyone. Many of the accounts are given a user id of zero, so that they execute with super-user permissions (Curry, 1990).

The problem with these accounts is that they open potential security holes. By not having passwords on them, and by having super-user permissions, these accounts practically invite crackers to try to penetrate them. Usually, if the cracker can gain access to the system, penetrating these accounts is simple, because each account executes a different command. If the cracker can replace any one of these commands with one of his own, he can then use the unprotected account to execute his program with super-user permissions (Curry, 1990).

Simply put, accounts without passwords should not be allowed on any UNIX system (Curry, 1990).

An account without a password is an easy target for an intruder and subjects the entire system to risk.

DII COE SRS Requirement:

3.2.1.1 The COE shall enforce individual accountability by providing the capability to uniquely identify each individual system user.

3.2.1.1.1 The COE shall require users to identify themselves before beginning to perform any actions that the system is expected to mediate.

3.2.1.2 Each user shall be identified by a globally unique user name or userID that will follow a standard set of processes or rules for formation.

3.2.1.3 The COE shall provide the capability of associating the user's identity with all auditable actions taken by that individual.

Test Actions:

Step: 1

Required Action:

In the "Program Manager", in the "Administrative Tools" group, select the "User Manager" icon. Verify that the "Guest" account has not been disabled and has a password.

Expected Results:

The Guest account has a strong password making it difficult for intruders to access the system.

Comments:

This should be done if some applications depend on the availability of "Guest" and cannot be rewritten not to depend on the Guest account. The extra protection is needed because "Guest" is a member of group "Everyone", which has modify rights on many Registry keys.

Topic: I&A

SubTopic: Password Management

Objective 111

Verify trivial passwords are not used for accounts.

Rationale:

Accounts should not use trivial passwords. Passwords that meet the requirements in the SRS help prevent an attacker from gaining access to the system.

DII COE SRS Requirement:

3.2.1.4 The COE shall use a protected mechanism (e.g., passwords) to authenticate each user's identity. If passwords are used as the mechanism, they shall meet the following requirements:

3.2.1.4.1 Passwords shall be at least eight alphanumeric characters in length.

3.2.1.4.3 The COE shall provide a graphical user interface (GUI) for selection of passwords.

3.2.1.4.4 The COE shall provide the capability for users, the SGSO, or the system to generate passwords only in accordance with specified selection rules.

3.2.1.4.5 Password selection rules shall be configurable by the SGSO. These rules shall include the following:

3.2.1.4.5.1 Maximum password age

3.2.1.4.5.2 Minimum password age

3.2.1.4.5.3 Password character set (e.g., alphanumeric plus special characters)

3.2.1.4.5.4 Minimum of one numeric character (i.e., 0-9)

3.2.1.4.5.5 Prohibit repeating characters (e.g., ee)

3.2.1.4.5.6 Dictionary words prohibited.

Test Actions:

Step: 1

Required Action:

In the "Program Manager", in the "Administrative Tools" group, select the "User Manager" icon. Select "Policies", "Account" from the menu. Verify that the "Password Minimum Length" is set to at least 8 characters. This setting will automatically disallow blank passwords.

Expected Results:

The "Minimum Password Length" should be set to at least 8 characters.

Comments:

Users should be trained to use alphanumeric and special characters in all passwords, use a minimum of one numeric character, not use any word that can be found in a book or dictionary (forward or reversed), and not use repeating characters in a password.

Step: 2

Required Action:

Interview the administrator. Verify that the administrator account password is a password that meets the requirements in the SRS (i.e. in the expected results).

Expected Results:

The "Administrator" account password is a password that meets SRS requirements (i.e. uses alphanumeric and special characters, uses a minimum of one numeric character, does not contain any word that can be found in a book or dictionary (forward or reversed), and does not contain repeating characters).

Comments:

The "Administrator" account has virtually unlimited user rights and cannot be locked out, and so needs exceptionally careful protection from access by unauthorized users.

Topic: I&A

SubTopic: Password Management

Objective 112

Verify password life is limited to a maximum of 180 days and the user is notified prior to password expiration.

Rationale:

Some UNIX systems allow the system administrator to set a "lifetime" for passwords. Users whose passwords are older than the time allowed are forced to change their passwords the next time they log in. If a user's password is exceptionally old, the system may prevent the user from logging in altogether (Garfinkel and Spafford, 1992).

DII COE SRS Requirement:

3.2.1.4.2 Password life shall be limited to a maximum of 180 days. The COE shall notify the user prior to password expiration.

Test Actions:

Step: 1

Required Action:

In the "Program Manager", in the "Administrative Tools" group, select the "User Manager" icon. Select "Policies", "Account" from the menu. Verify that password age is set to 180 days.

Expected Results:

In the Maximum Password Age list box the password age should be set to 180 days.

Comments:

Regularly changing passwords limits the length of time a password obtained by an attacker can be used and limits the likelihood that a departed employee will still have access to the system. The tradeoff is that if the expiration time is set too short, users will either forget the new password or write it down.

Step: 2

Required Action:

In the "Program Manager", in the "Administrative Tools" group, select the "User Manager" icon. Select "Policies", "Account" from the menu. Verify that passwords can not be reused until 10 other unique passwords intervene.

Expected Results:

In the "Password Uniqueness" list box, 10 other unique passwords should be set.

Comments:

This setting makes it more difficult for users to bypass the requirement to change passwords by immediately resetting the password to the original value.

Step: 3

Required Action:

In the "Program Manager", in the "Administrative Tools" group, select the "User Manager" icon. Select "Policies", "Account" from the menu. Verify that changing a password immediately after it is set is disallowed.

Expected Results:

The "Minimum Password Age" is set to at least one day.

Comments:

Makes it more difficult for users to bypass the no-reuse restriction.

Topic: I&A

SubTopic: Mandatory profiles for shared user Ids

Objective 286

Verify that mandatory profiles are configured for shared UserIDs.

Rationale:

Shared UserIDs are a violation of security.

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

Interview the System Administrator to determine if shared user Ids are being used, and if so, if mandatory profiles are being used.

Expected Results:

Shared user Ids are NOT being used as this is a violation of User Identification and Authentication.

Comments:

For more details, see the NTAS System Guide, Chapter 14.

Do this if userIDs are used by several human users and the site is configured as a domain.

Users with mandatory profiles cannot permanently change the desktop.

Topic: I&A

SubTopic: User Accounts

Objective 266

Verify that the name of the administrator account has been changed from "Administrator" and is kept secret from non-privileged users.

Rationale:

The Administrator account has virtually unlimited user rights and cannot be locked out. Changing its name to one that is a closely held secret makes it more difficult for an attacker to determine the password.

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

In the "Program Manager", in the "Administrative Tools" group select the "User Manager" icon.

Expected Results:

The "Administrator" user does not appear in the user list displayed.

Comments:

Step: 2

Required Action:

In the "Program Manager", in the "Administrative Tools" group, select the "Regedt32" icon. Click on the window "HKEY_LOCAL_MACHINE" and the folder "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon".

Expected Results:

The "DontDisplayLastUserName" key is set to "1".

Comments:

This protects the name of the administrator from being obtained.

Topic: I&A
SubTopic: Accounts

Objective 102

Verify there are no guest accounts on the system.

Rationale:

Guest accounts present a security hole. By their nature, these accounts are rarely used, some are always used by people who should only have access to the machine for the short period of time that they are guests. The most secure way to handle guest accounts is to install them on an as-needed basis, and delete them as soon as the people using them leave. Guest accounts should never be given simple passwords such as "guest" or "visitor," and should never be allowed to remain in the password file when they are not being used (Curry, 1990).

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

In the "Program Manager", in the "Administrative Tools" group select the "User Manager" icon. Then double-click on the user "Guest".

Expected Results:

The "Account Disabled" box IS checked in the "Guest" "User Properties" dialog box.

Comments:

The "Guest" account is a known user ID on Windows NT systems and, as installed, does not require a password. "Guest" is a member of the group "Everyone" and has all the rights associated with this group. This is a vulnerability because many Registry key ACLs are set to "allow modify permissions" for the group "Everyone". The Registry cannot be secured because it is too large and complex to allow definitive identification of keys that should not be modifiable by the group "Everyone". In addition, write and delete permissions for the group "Everyone" are needed by some keys.

Step: 2

Required Action:

Verify that if the "Guest" account has not been disabled, the "Guest" account user rights have been restricted to the least needed.

In the "Program Manager", in the "Administrative Tools" group select the "User Manager" icon. Then double-click on the user "Guest". Select "Policies", "User Rights" from the menu. Select each right one at a time from the "Right" dropdown list and view the users granted the chosen right.

Expected Results:

The user rights for "Guest" have been restricted to the "Access this computer from network" right. In particular, "Guest" should NOT have the "Log on locally" right.

Comments:

Removal of the "Log on locally" right, prevents "Guest" users from accessing the system except from the network, and limits the system vulnerability. However, any "Guest" can run "regedt32" over the network and attack the Registry. Using these recommendations limits to some degree the damage that can be done if an attacker accesses the system as "Guest".

Topic: I&A
SubTopic: Accounts

Step: 3

Required Action:

Verify that any system on which the “Guest” account is enabled, with or without a password, is isolated as much as possible from the rest of the network and is not trusted by other systems on the network. Any system on which the “Guest” account is enabled is vulnerable to attacks on the Registry.

Comments:

Topic: Markings

SubTopic:

Objective 6

Verify a security warning is displayed prior to the login process indicating restrictions that apply to logins, the highest classification of information processed on the system, and that misuse is subject to applicable penalties.

Rationale:

DII COE SRS Requirement:

3.2.7.1 The COE shall display a security warning prior to the login process that indicates the highest classification of information processed on the system and that misuse is subject to applicable penalties.

Test Actions:

Step: 1

Required Action:

View the monitor prior to login.

Expected Results:

A security warning is displayed prior to the login process indicating restrictions that apply to logins, the highest classification of information processed on the system, and that misuse is subject to applicable penalties.

Comments:

Topic: NETWORK CONFIGURATION

SubTopic: Network Services

Objective 268

Verify that DHCP (Dynamic Host Configuration Protocol) has been deleted.

Rationale:

DHCP (Dynamic Host Configuration Protocol) dynamically reassigns IP addresses. Any security features that rely on IP addresses to identify hosts, such as some firewall systems, will be less reliable if DHCP is used.

DHCP is not used for C2 configuration.

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

From the "File Manager" select the "C:\WINNT35\SYSTEM32" directory and determine if the "DHCP" directory exists.

Expected Results:

The "DHCP" directory does not exist.

Comments:

Topic: NETWORK CONFIGURATION

SubTopic: Network Services

Objective 269

Verify that the Windows Internet Name Service (WINS) has been deleted.

Rationale:

WINS is not used in C2 configuration, and any unnecessary complexity of the operating system potentially increases vulnerability, therefore, this additional operating system capability should be removed.

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

From the "File Manager" select the "C:\WINNT35\SYSTEM32" directory and determine if the "WINS" directory exists.

Expected Results:

The "WINS" directory does not exist.

Comments:

Topic: PHYSICAL PROTECTION

SubTopic:

Objective 186

Determine if the proper physical protections are used.

Rationale:

Access to the domain controller is required for most user activities and becomes a major single point of failure. Domain controllers are a single point of attack for user capabilities. If any account with administrative rights is compromised, the attacker can change rights of any user on network.

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

Verify that critical systems are physically protected so attacker cannot replace BIOS or drain BIOS battery or carry away disk drives.

Expected Results:

Systems are physically protected.

Comments:

Physical access can be used to bypass Windows NT security features.

Step: 2

Required Action:

Verify that removable media is stored in a physically secure location. Train system administrators and users that data on floppy disks and backup media is NOT protected by file system security.

Expected Results:

Backups and floppies are handled securely.

Comments:

Data on removable media (i.e. backup tapes and floppies) is not protected by Windows NT 3.51 file access controls. A backed up file can be restored to a volume that does not have security enabled, on any system; therefore, backups must be controlled.

Topic: SYSTEM ARCHITECTURE

SubTopic:

Objective 147

Verify the Security Services maintain a domain for their own execution that protects them from external interference or tampering (e.g., by modification of their code or data structures).

Rationale:

DII COE SRS Requirement:

3.2.14.1 The COE Security Services shall maintain a domain for their own execution that protects them from external interference or tampering (e.g., by modification of their code or data structures).

Test Actions:

Step: 1

Required Action:

If the site has many Windows NT workstations verify that if the site is configured as a domain, a primary domain controller and a backup domain controller are available.

Expected Results:

Comments:

This is recommended if the site has many Windows NT workstations. User account maintenance in a Workgroup configuration requires visiting each workstation, while user account maintenance for a domain can be performed from a central location. Users can log into single account, with their own desktop environment, from any WinNT system on the network. In addition the system holding the SAM database can be protected more stringently than is convenient for user workstations.

Topic: SYSTEM ARCHITECTURE

SubTopic:

Objective 158

Verify the user environment is configured properly. For instance in UNIX systems, by default, the /etc/profile file sets the user terminal type, checks for new email, and sets the umask. Any other activity should be explicitly approved.

Rationale:

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

In the "Program Manager", in the "Administrative Tools" group, select the "Regedt32" icon. Click on the window "HKEY_CLASSES_ROOT". Select "Security", "Permissions" from the menu.

Expected Results:

Verify that permissions on "HKEY_CLASSES_ROOT" and all its subkeys are set to:

Administrators: Full Control
Creator/owner: Full Control
System: Full Control

Comments:

These settings protect against an attacker changing the binding between file extensions and applications. Changing bindings could increase the risk of execution of Trojan Horse programs. The impact of these settings is that only members of the "Administrators" group may be able to install some software packages.

Step: 2

Required Action:

In the "Program Manager", in the "Administrative Tools" group, select the "Regedt32" icon. Click on the window "HKEY_CLASSES_ROOT". Select "Security", "Permissions" from the menu.

Expected Results:

Verify that permissions on "HKEY_USERS\DEFAULT\UNICODE Program Groups\[all subkeys]" are set to:

Administrators: Full Control
Everyone: Read

Comments:

These settings protect the bindings between an icon and its program pathname. Changing the binding could increase risk of execution of Trojan Horse programs. The impact of these settings has not been fully investigated. Other trusted groups such as "Power Users" could be given "Full Control" access.

Step: 3

Required Action:

In the "Program Manager", in the "Administrative Tools" group, select the "Regedt32" icon. Click on the window "HKEY_LOCAL_MACHINE". Select "Security", "Permissions" from the menu.

Expected Results:

Verify that permissions on "HKEY_LOCAL_MACHINE\Software\Microsoft\RPC\[all subkeys]" are set to:

Administrators: Full Control

SYSTEM: Full Control

Topic: SYSTEM ARCHITECTURE

SubTopic:

Creator/owner: Full Control

Everyone: only Query Value, Enumerate Subkeys, Notify, and Read Control

Comments:

The impact of leaving the default permissions for Everyone that allow Everyone to modify the RPC keys has not fully been analyzed; however, the suggested settings appear to provide useful protection without damaging functionality.

Step: 4

Required Action:

In the "Program Manager", in the "Administrative Tools" group, select the "Regedt32" icon. Click on the window "HKEY_LOCAL_MACHINE". Select "Security", "Permissions" from the menu.

Expected Results:

Verify that permissions on "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\[all subkeys] are set to:

Everyone: Query Value, Enumerate Subkeys, Notify, Read Control

Comments:

Step: 5

Required Action:

In the "Program Manager", in the "Administrative Tools" group, select the "Regedt32" icon. Click on the window "HKEY_LOCAL_MACHINE". Select "Security", "Permissions" from the menu.

Expected Results:

Verify that permissions on "HKEY_LOCAL_MACHINE\Software\Windows3.1Migrations Status\[all subkeys]" are set to:

Everyone: Read.

Comments:

This subtree contains WinNT configuration information. This change may make it impossible for users not members of the Administrators group to install some software packages.

Step: 6

Required Action:

In the "Program Manager", in the "Administrative Tools" group, select the "Regedt32" icon. Click on the window "HKEY_LOCAL_MACHINE". Select "Security", "Permissions" from the menu.

Expected Results:

Verify that permissions on "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Profile List are set to:

Administrators: Full Control

SYSTEM: Full Control

Creator/owner: Full Control

Everyone: Special Access (Query Value, Create Subkey, Enumerate Subkeys, Notify, Read Control)(i.e., Turn off the Set Value permission.)

Comments:

These settings allow caching of profiles while preventing an attacker from changing the filename pointing to a user's profile. An untested enhancement would be to replace "Users" with the special group "INTERACTIVE". This would prevent an attacker from creating a Trojan key for a user who is not logged on.

Topic: SYSTEM ARCHITECTURE

SubTopic:

Objective 188

Verify security support tools are provided to periodically determine the security posture of systems, to validate the strength of the authentication mechanism, and to determine changes to designated systems and application files.

Rationale:

DII COE SRS Requirement:

3.2.15.6 The COE shall provide the SGSO a standard set of security support tools to periodically determine the security posture of COE systems.

3.2.15.6.1 The COE shall provide the capability to validate the strength of the authentication mechanism. For example, the capability will check for potentially weak passwords.

3.2.15.6.2 The COE shall provide the capability to determine changes to designated systems and applications files, e.g., password or rc.* files.

Test Actions:

Step: 1

Required Action:

Verify that the system administrator has access to the WinNT 3.51 system documentation and to the Windows NT 3.51 Resource Kit. Specifically, the tools Computer Profile Setup (CPS) and the C2 Security Configuration tool (C2Config) should be available.

Expected Results:

Comments:

Although administering a Windows NT system is much easier to administer than a Unix system, it still requires some expertise. Unless it is maintained, the security configuration established at installation will degrade over time.

Step: 2

Required Action:

Verify that a current virus protection program specific for Windows NT and capable of checking for macro viruses is available on the system.

Expected Results:

A virus protection program is installed.

Comments:

Note: Anti-virus programs need to be updated regularly.

VirusScan for Windows NT

McAfee Associates, Inc.,

2710 Walsh Avenue, Santa Clara, CA 95051.

Telephone: 408-988-3832

Fax: 408-970-9727

To Download McAfee Products

BBS: 408-988-4004 (Settings: 8,N,1 Speed: Up to 28.8K)

Internet FTP: ftp.mcafee.com

WWW: http://www.mcafee.com

CompuServe: GO MCAFEE

America Online: MCAFEE

The Microsoft Network: MCAFEE

NOTE: VirusScan for Windows NT 3.5.1 does not install on an NT Server!

Topic: SYSTEM ARCHITECTURE

SubTopic:

F-PROT Professional for Windows NT.

Data Fellows Inc.

4000 Moorpark Avenue, Suite 207

San Jose, CA 95117

tel (408) 244 9090

fax (408) 244 9494

URL: <http://www.datafellows.fi/f-prot/prodinfo/fp-nt.htm>

Norton Anti-virus for NT by Symantic, <http://www.symantec.com/>

While viruses specifically designed for Windows NT systems are not yet common, viruses are still a risk for Windows NT systems. Some MS-DOS viruses can do damage to a Windows NT system, and as Windows NT becomes more widespread, viruses designed for Windows NT will become more common.

Step: 3

Required Action:

Verify that the tool DumpReg is available to the system administrator.

Expected Results:

Comments:

DumpReg generates a report showing Registry key ACLs. DumpReg is available from "<http://www.somarsoft.com>".

Step: 4

Required Action:

Verify that the tool DumpAcl is available to the system administrator.

Expected Results:

Comments:

DumpAcl generates a report showing file ACLs. DumpAcl is available from "<http://www.somarsoft.com>".

Topic: SYSTEM ARCHITECTURE

SubTopic: Admin Tool Authorization

Objective 144

Verify that only authorized users are able to perform administrative tasks that can effect system security.

Rationale:

Many administrative tools can enhance the exploitation process if executed by someone who is trying to exploit the system.

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

Verify that only users explicitly approved for performing backups, specifically excluding the Administrators group, have the right to backup files.

In the "Program Manager", in the "Administrative Tools" group, select the "User Manager" icon. Select "Policies", "User Rights" from the menu. Remove "Administrators" from and add either the group "Backup Operators" or specific users to the right "Backup files or directories".

Expected Results:

In the "User Rights Policy" dialog box, "Administrators" has been removed. The group "Backup Operators" or specific users have been added.

Comments:

Use of the backup right grants access to all files, because a backed up file can be restored to a volume that does not have security enabled, such as a FAT filesystem, on any system, and use of this right bypasses all discretionary access control checks. Although Administrator can take ownership of any file and thereby gain access, the act of taking ownership is audited. Exercise of the backup right is not audited. Limiting the backup right to specific users increases the traceability of these file accesses.

Step: 2

Required Action:

Verify that only users approved for performing backups have the backup right.

In the "Program Manager", in the "Administrative Tools" group, select the "User Manager" icon. Select the "Policies", "User Rights" from the menu.

Expected Results:

Only users approved for performing backups have the backup right.

Comments:

A backed up file can be restored to a volume that does not have security enabled, such as a FAT filesystem, on any system; therefore, backups must be controlled. Users with the backup right can bypass all DACL checks.

Topic: SYSTEM ARCHITECTURE

SubTopic: Operating System

Objective 153

Verify the appropriate operating system patches have been applied.

Rationale:

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

Expected Results:

Windows NT Service Pack 4 should be installed.

Comments:

Windows NT as delivered is not a secure system. Service Pack 4 configures the system for C2 security. While Service Pack 4 may impose controls more stringent than required or desired, it is safest to first over-tighten the system, then loosen specific controls as required.

Service Pack 4:

The file sharing service if available and accessible by anyone can crash the NT machine and require it to be rebooted.

This vulnerability is documented in Microsoft Knowledge Base article number Q140818 last revision dated March 15, 1996. Resolution is to install the latest service pack for Windows NT version 3.51. The latest service pack to have the patch is in service pack 4. source: Christopher Klaus <cklaus@iss.net>, 21 May 1996.

Topic: SYSTEM ARCHITECTURE

SubTopic: Operating System

Objective 152

Determine the OS version installed. Verify that it is the correct version.

Rationale:

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

During installation modify disk partitioning and formatting to remove any other operating systems.

Expected Results:

Windows NT is the only operating system installed on the system.

Comments:

If the system can be booted into MS-DOS or LINUX, all Windows NT security features can be subverted. This includes the file system controls, since a program that runs under DOS that can access an NTFS filesystem is publicly available on the Internet. If the system can be booted into a version of Windows NT that has not been configured as described in this document, some of the configured security features can be bypassed.

Omitting a second operating system from the hard drive does not provide complete protection, since it does not protect against booting from an MS-DOS floppy, but it is a desirable precaution.